National College of Ireland

Suggesting and Evaluating Antivirus Performance to Secure Application Server

MSc Research Project
Cloud Computing

Niharika Vashishtha
Student ID: x21153213

School of Computing
National College of Ireland

Supervisor: Aqeel Kazmi

National College of Ireland
Project Submission Sheet
School of Computing

National College of Ireland

Student Name:	Niharika Vashishtha
Student ID:	x21153213
Programme:	Cloud Computing
Year:	2022
Module:	MSc Research Project
Supervisor:	Aqeel Kazmi
Submission Due Date:	01/02/2023
Project Title:	Suggesting and Evaluating Antivirus Performance to Secure Application Server
Word Count:	8080
Page Count:	25

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Niharika Vashishtha
Date:	29th January 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Suggesting and Evaluating Antivirus Performance to Secure Application Server

Niharika Vashishtha
x21153213

Abstract

Cloud Computing opens the door for the advancement of innovative technologies with ease of development by providing already built-up innovative ideas. However due to completely based on internet it snitches attentions of attackers. The business of any organization can be affected if attackers find security related loopholes in the application and cause serious harm. These attacks can be due to outsider or insider of the organization. Antivirus can be a solution to deal with such issues. Antivirus software can find vulnerabilities, detect malicious files, report them to the administrator and ask them to delete. These antiviruses keep updated for any new signature. In this research some freely available antiviruses are selected that can be used as a defensive mechanism to protect the operating environment in cloud. The study is conducted for Ubuntu EC2 instance and Window's EC2 instance. After installing the select antivirus the environment is fed with malicious data and then scanning by each antivirus has been done. This detailed research not only focuses on the scanning result provided by the antivirus but also finds the performance of the software during scanning. These overall results can be helpful for the cloud users to select one of the solutions based on their business requirements. CloudWatch service of AWS is used to monitor the performance. In the end, a conclusion is made in which all the findings are discussed and how performance-related problems can be solved is addressed.

1 Introduction

Cloud computing is popular among businesses due to its high availability and scalability. Today's world is of intense competition and business wants its application to be reachable all the time to its users without any downtime even the business expectation is to accommodate users at the time of rush hours. Cloud computing proves to be the best internet use over a long time, giving cost-effective solutions. While getting tremendous amounts of benefits, most of the businesses feel a little insecure to shift their business to a place where information can be easily hacked. Hybrid cloud is an option for bigger businesses but for small Enterprise public cloud offers multiple benefits. By choosing public cloud for their application to run, it is to be taken into consideration that the security policies are in the benefits of the business, no loopholes are remained to get open to invite hackers.

1.1 Motivation

Security of the application is an especially crucial factor that cannot be ignored. Cloud computing is very innovative, easy to learn and easy to implement technology when used appropriately. Some evidence is presented here which motivates me to do this research.

According to one article published in the year 2021, by migrating only a mailing infrastructure to cloud, or taking the mailing service available in the cloud can invite more intruders and attackers from outside. This research raises the question of using cloud services and loss of business due to these kinds of scenarios. Dey et al. (2021)
All Cloud providers ensure safety by giving the proper advice about how to handle it using strategy and policies and managing ownership and accountability of any future risk happened to the system in using services. Through Network security handling a zone approach can isolate each application or instances in cloud from each other. By having Identity Access management, a role and authority access management can be done. Encrypted data is needed at store as well as when it is in transit and most important continuous monitoring and alerting job for all environments and instances.

Above discussed security measures need to be applied for a secure environment but after doing all these there is a chance that malware can cause harm to the system and cost the business. Therefore, using antivirus protection to protect the environment and running instances can be a solution.

Antiviruses are software solutions to provide safety from virus attacks and multiple kinds of malware. Attackers are continuously enhancing the quality of viruses and find the way to improve so they can pass the security check do the harm to the machine or take the benefit of the situations in any ways. It is said that once an intruder attacks the system the application is not yours anymore as it shows unexpected behavior which is for some time not into your control. To fight against continuously updating virus industry the antivirus solution should be smart enough. This leads me to check the performance of antivirus on cloud platforms to determine which antivirus is good enough to protect the application.

1.2 Research Question:

How to enhance security on application servers by measuring the performance metrics of different antivirus on a cloud environment?

1.3 Objectives

The objectives of this research are:

- To find suitable antivirus solutions for both Linux as well as Windows operating environment that can enhance security mechanism of a cloud hosting application.
- To evaluate the performance of selected antivirus solutions on defined criteria or conditions, provide unbiased results and discuss all aspects encountered during research. This research will evaluate the result on the following criteria.
  - **Virus Detection:** A good AV should be able to scan and identify viruses in the system, irrespective of the operating system on which it installed.

  - **Faster and less-resource consuming:** AV should be lightweight, so that, not only takes less time to scan but consume less CPU resources at time of scanning. If an application is heavy contents like images and videos streaming, Antivirus should not slow the performance of the application.
  - **User Friendly:** Antivirus should be easy to use and able to give signal as soon as found threat.
  - **Configurable:** Antivirus should be configurable according to requirement. It can be manageable and schedule able. Cron job can be written to guide the antivirus like run at the required time, scan only specified folder, not take full control of the system.
  - AV should have enough features for your application.

- After getting result discuss the impact of using a selected solution and how it will affect the environment and how to deal with under-performing solution if found it is an effective tool to fight against virus and vulnerabilities.

2 Related Work

Cloud Computing offers multiple benefits to its users in effective cost. This is the reason behind increased business are moving towards cloud to spread in the world using internet. The in-built services provided by the cloud reduce development costs and provide a better service. On one hand cloud give these services in minimal charges and on other hand using public cloud can be a challenge itself. Businesses are sometimes aware of these challenges and afraid to come on cloud. Cloud providers offer multiple services to secure the environment and monitor it to check the performance and user activities. Still attackers can find the security hole and benefit from it if found unprotected. These attacks can be malicious attacks and can be handled by installing antivirus as a security mechanism.

2.1 Cloud Computing and factors to be considered

In recent scenarios Cloud computing has been marked as one of the most important resources of any organization. Cloud computing ensures providing efficient and scalable solutions in defined cost. Organizations face challenges like data management, storage, integrity, security, and speed. These can be sorted out by switching to cloud. Computation on big data set needs for high performing and big storage machines. The studies show that cloud computing gives better management to handle all the business needs. Yoo and Kim (2018). Small businesses find it easy and relevant to move, which reduces their cost of infra and adds more security in minimal maintenance environment. As more businesses are going to be clouded daily, it is important to improve the security around it. Data related to any organization is important and should be protected. Since clouds are a distributed architecture, it is possible to face many attacks from different attackers. Many cyber criminals can cause data theft, DoS (Denial of Service) attacks and many other things like unauthorized access. Public clouds are more prone to face such problems. The providers of cloud services are concerned about the security but not guarantee about the theft if happened, in such cases they suggest incorporating more security measure before deploying application. Cryptographic encryption can handle these problems, but

a single level of cryptographic encryption can be broken easily by smart attackers. In some studies, the possible solution is applying multi-level of encryption which can make system less vulnerable to access. Sharma et al. (2019)

2.2 Security Risk Evaluation

Cloud tenancy encourages identifying security issues that can impact the overall performance and impact on business. For example, in the overall life cycle of a product the architecture of software should be the same in every stage, similarly identifying the risk and threats related to product development should be an umbrella activity. Sgandurra and Lupu (2016) As technology is growing, methods to attack and threats are also evolving. Some risk evaluation models not only evaluate the potential system threats but also propose tailored countermeasures to control them. The cause-consequences are evaluated before, and we find the probability that a threat can be caused and loss due to it. Nhlabatsi et al. (2018)

Security measures applied to any organization must be configured on each device, and this can be an overhead. There are some configurations that hardly change into its lifecycle is good to be employed but some changes, which need to be updated in regular duration and require manual interaction become hard to be corrected in one go. The static changes that are constant in overall development of project is easy to maintain, on the other hand the frequent changes are good to be observed at every stage of the project life cycle and determine the vulnerabilities and tell the hosting providers. The user needs to set a boundary and take an evaluation to check provider's security levels for an application to host on shared resource. Provider can be fully responsible for the security if the application is SaaS. However, if user is getting a service for IaaS and PaaS (Platform as a Service), all the intrusions and attacks need to be addressed and measures need to be taken beforehand. Carstensen et al. (2012)

2.3 Antivirus Protection

It is clear from the above discussion that security measures should be considered before going towards cloud computing, especially in a multi-tenancy environment. Even it is possible that quantum computers can be affected by the harmful circuits. These can be protected by the pattern matching feature of the antivirus. Deshpande et al. (2022)

To check the vulnerability issues in windows operating system using in cloud EC2 research is experimented with some configuration like wide-open and out-of-the-box. Both experiments are to test security of operating system in cloud. In a wide-open scenario, all opened ports belong to a single machine so that machine can get attentions of increasingly malicious attackers to measure vulnerability of machine, when no security measures are applied. While in out of box experiment only few default ports and services are opened. In both the experiments the attackers in very few minutes found vulnerabilities in the system and attacked the malicious files. This research concluded that every machine connected to the internet is scanned whether the ports are opened or not, while opened ports machines are more vulnerable, and can get more exploitation attempts. Mostly exploitation requires involvement of the client. So, applications, open for all users can invite attackers to the system by just a simple click. Zeng et al. (2014)

To find and achieve new goals of high performing applications, both small and big budget businesses are moving to distributed cloud. This enables criminals to be increas-

ingly vigilant about using malware to harm the products and use them to gain profits for themselves. To limit cyber-attacks antivirus are considered as a satisfactory solution. This leads to growth of the antivirus market and according to one report this will rise to 10.8%. Updates (2021).

As cloud computing is growing and using its power to scale the current system or process, Antivirus software solutions find it efficient to deploy in the cloud and use it as a service to provide an additional layer of security. Antivirus programs have limitation of consuming too much memory and CPU usages, which eventually affects performance of systems as well, but this limitation can be eliminated by going towards the in-the-cloud antivirus solutions. Even present cloud-based antivirus systems can be enhanced by implementing data-mining techniques. Agrawal and Wahie (2016)

2.4 Malware detection in cloud

To protect the system, Antivirus is not a recent technology to rely on. Malware protection in cloud, is necessary to protect the organization's data and application from outsider attacks. In research a malware detection system in cloud is installed such that it can provide better malware detection. It uses multiple antivirus software to combine to create an environment which can give better results, against recent threats by applying static as well as heuristic techniques to detect malware. Also, this research uses FTP to alert the user about the malware and it will allow a normal desktop user, whose system is connected through cloud to receive the benefits of cloud. Hatem et al. (2014)

In research the proposed solution is comprised of some VM hosts, DNS, webservers, SMTP and eight physical workstations. These workstations run five windows VMs. Physical machines are isolated from the internet and Virtual Machines and in this way virtual hosts are using endpoint protection of McAfee. This is the architecture to protect and build web security, mail security, and configure firewalls. This service is transparent and gateway router presented in internal network allow incoming traffic to go through the McAfee and imperva servers while going to the production network, this will protect against any threat to enter the network. This solution is then compared to the traditional security solutions provided for personal computers and found the solution is cheaper. Salah et al. (2012)

One of the research projects is pointing towards the solution provided by experimenting on VirusTotal and comparing it with the desktop Antivirus detection solutions. The methodology used in this paper for the evaluation is to generate malware that must be detected by both desktop as well as VirusTotal solution. This assessment is needed to identify the authenticity of Virustotal because the platform is used widely to determine the efficiency of antivirus software. The performance of both the desktop and VirusTotal version is checked using some scenarios first is to find the malicious file in both version second is at which stage it is found like download, scan or execute stage and third is to identify the samples when the cloud is used that is the use of cloud for each AVs can affect the decisions. This research is important to check the discrepancies between the Virus total versions and how different antivirus are using this platform to detect viruses. Leka et al. (2022)

To make virus detection more efficient an architecture proposed in the research is making a system where home cloud server is connected to the multiple sub-servers, in each sub servers one terminal is running and checking the files received from the sub server one by one and identifying the virus signatures. After scanning the files, the files

declared as infected or not infected. Each sub-server is checking for a particular signature. This research focused on optimization of the process of virus detecting method. Memos and Psannis (2015)

No matter which operating system you choose when creating the instance, it can be affected by the virus, but if follow the statistics Linux machines are less affected by malware. This is one of the reasons behind the selection of Linux as an instance in many organizations but if it is affected by malware the applications will change the behavior and may cause trouble.

In this research by analyzing multiple antivirus behavior the findings tell that every antivirus act differently depending upon the program for which it has been written, so it is suggested to install more than one antivirus to protect from different malware. But the problem with this solution is that at the run-time antivirus can interact and can attempt to block each other from performing and performance can be impacted by antivirus as well as of machines. The performance evaluation is done by identifying some if the metrics and by constantly observing the behavior of installed antivirus. Raffa (2021)

Antivirus provides malicious and threat protection to the machine, but hackers are using evasion tools to evade antivirus. This research evaluates some defined evasion tools like Phantom-Evasion, Shelter, Hercules against some top antivirus solutions. In this way this research somehow evaluates the effectiveness of antivirus solutions. Penetration tester also used this kind of tool to find the effectiveness of the antivirus solutions. In the research at first, list of antiviruses is selected using reviews of antivirus and some free antivirus then host machines are set with windows8 64bit processors and two virtual machines are made one for attacking machine and one for targeting machine. The evasion tools are then installed on attacking machines and malware samples are generated which then deployed on the target machine. One by one antivirus solutions are installed and tested for malware samples. If an antivirus solution found the virus some score is awarded. The implementation is not yet done of this research. Garba et al. (2019)

Generally, in any organization a mixture of operating systems is available. In such scenarios, it is important to have an antivirus which can find malware in multiple operating systems or combination of antivirus is needed to handle such conditions. This concern is raised in the research paper by Stange (2015).

In this research they collected samples of malware scan results of different antivirus and listed them with the results when multiple antivirus works together to scan the entire system. The interesting result is found that the antivirus program written for Linux system is caught to find the malware in Windows and Android system and multi scanning option gives best results.

Different payloads are tested with the help of antivirus. It is found in the research that the module created named Metasploit attack can be efficiently handled by the antivirus software. It is found that it may not be an effective technique to test the antivirus program instead the combination of tests should be performed to test the antivirus because malicious attack is continuously changing the effectiveness of antivirus is evolving with this. One kind of test cannot guarantee its effectiveness. Casey et al. (2019)

This research is focused on the performance of freely available tool Sysmons. This tool logs the critical events that happen in Windows environment. It is also sent those to further analysis and understand. It is found that this is a usual behavior that some malware can easily bypass the security scan of anti-viruses by analyzing the behavior of antivirus the gap can be closed by providing useful recommendation that can be adopted to identify malicious activity in the system. In this way the weakness of antivirus software

can be compensated. Ongaro (2020)

To identify the correct solution for malware intrusion in a paper Santos (2021) concluded that the paid antivirus protection is better for finding the malware in the system compared to free antivirus. The paid software scans a larger area of the system, so they take a lot of time to search through each area, which may result in better findings but ample amounts of time and CPU power. Some antiviruses, however, can choose from quick, full, and custom scan. The experiment is conducted using ransomware simulator and Eicar test files.

There is a tool HEAVEN stands for Hardware-Enhanced AntiVirus Engine that improves performance of antivirus used into x86 processor and MS Windows operating system. It uses both hardware and software to enhance performance. HEAVEN is tested with approx. 10,000 malware samples and many software samples and improved the malware detection rate and reached 100% without any false positives. It effectively decreased the CPU cycles for scanning and memory throughput and even disk writes and disk reads. HEAVEN works by identifying the common features in malware and saving it for future reference. The performance of HEAVEN is evaluated by analyzing how efficient signature it generated for a malware, how effectively it then detects malware and how it enhances the performance, it also gives some results on False Positive results calculated by antivirus. Botacin et al. (2022)

3 Methodology

The study is focused on the performance of antivirus on Ubuntu and on windows cloud instances. To test the antivirus, first there is a need to identify the different antivirus for these servers. The antivirus work on different methods to detect the threat in to the system.

- **Static Analysis:** In static analysis static properties of data is checked. After viewing, gathered information can be helpful in identifying that the data may corrupt and cause problems to the system. These properties can be seen by just viewing the metadata, if the file found corrupted into static analysis deep investigation may be done by the antivirus software. This is the very first stage in any antivirus to determine the next stage taken by the software.

- **Behavior Analysis:** Antivirus software do behavior analysis of the data sample by interacting with the system. In behavioral analysis using automated tools the capability of malware is analyzed. In a virtualized safe environment, the suspected malicious code is tested to find the type of malware as well as the potential harm the sample can do.

- **Automated Analysis:** In this type of analysis technique the suspicious file is analyzed for potential repercussions it can cause to the network. It uses an automatic technique to find the malware in a faster way.

- **Cloud Antivirus Detection:** Cloud antivirus detection is used cloud support and this is why uses internet connection. Instead of installing complete package on the operating environment this technique uses network connection between the machine and cloud where antivirus is working. In this way it supports the application server performance by not running antivirus software in local.

- **SandBox Detection:** Sandbox detection is a separate platform where suspected files or program are send to run and check the behaviour, if in test it shows unexpected or any harmful behaviour then notification is send in response.

- **AI techniques:** Machine learning or Artificial Intelligence technology is used to identify such files that can possibly do the harm to the system. with

The available antiviruses use the same methodologies to scan for the virus and detect them. Antivirus use their available database to match the signature of virus and declare them as infected file. Based upon the different techniques used to find the virus the performance of different antivirus software solutions can be different. Mostly software uses combination of above mentioned techniques to effectively detect harmful viruses.

However, it is necessary that antivirus should contain at least some of the basic properties, such as:

- **Detection:** As antiviruses are designed and used to search the malware in the system, it is necessary for them to identify the malware in the system as soon as they scan.

- **Speed:** Antivirus should be fast enough. It is an important property that how fast an antivirus can detect the virus and give the response. It is possible when antivirus software keeps updating themselves for new malware. A faster detection is necessary to identify a potentially harmful file, before they run and do any damage.

- **Performance:** A good antivirus performance is not only based upon how fast it can identify various viruses but also depends upon how much CPU resources it consumes while scanning the system. If an antivirus is taking too much CPU resources, it can slow down the other running procedure because the scanning for virus comes into high priority task. An effective antivirus who uses lesser CPU resources can be used with other running applications.

- **Smart:** An antivirus must have sufficient features for the task it will going to do in an effective way, for example if it is doing signature matching to identify malware and in local database signature is not found, it should be fast enough to check the cloud database. Depending upon the application, one can choose the type of antivirus.

Based on these characteristics the list of antiviruses for this research is selected, so that effective comparison between them can be made. As Linux and Windows are both completely different platforms, it is not possible to find the same antivirus solution that can work on both servers and this research is about to evaluate available antivirus in the Cloud environment. The antivirus named below and tested in this research These listed antiviruses are freely available to install.

- **For Ubuntu:**

  - **ClamAV:** ClamAv is an opensource and free available antivirus solution available for Linux instance. It can detect various kinds of viruses including trojan, signature-based viruses and many malicious threats. Clamav allows us to modify configurations and use its best features accordingly. for example, one

can set clamav daemon and it will allow clamav to run in the background and always do the scanning. Clamav is widely used software in many organizations, one of the reasons for its updated database.

- **Sophos:** Sophos antivirus is a software solution available for free for Ubuntu. It provides malware scan and sometimes cleans the harmful threats. It matches the signature-based pattern and uses AI threat detection techniques to detect the virus.
- **RootKit Hunters:** Rootkit Hunter is another kind of Antivirus program often used to find rootkits, local exploit alerts and any suspicious activity in the system. Rootkit hunters scan the complete system at once and scan all the files as well as hidden files. It checks and warns users if any vulnerabilities are found in the system by generating warning alerts. It uses its database and matches all the files present in the system by comparing the available database and in the log provide all the details related to any threats and security breaches found in the Linux system. The user can change the configuration files after installing it on the machine as well as update the database of RootKit Hunter so that the antivirus can give the right result.
- **COMODO:** COMODO is another antivirus available freely for Ubuntu users. It protects the machine from viruses like trojan horses, worms and other malware. It can detect and block virus when find it in scan and sometimes remove it.It is an easy to configure software one can write cron jobs for it and to schedule time-based scanning. The antivirus solution can provide safety from email viruses. The virus database of COMODO is updated regularly to provide better protection. COMODO is GUI based system to use it from terminal.
- **F-Prot:** F-prot is an antivirus for Linux operating machines. F-prot gives many configurations related choices. F-prot scan for each file and search for macro viruses and if malicious software is present in the machine. It has powerful scanning. One can set cron statements to schedule the scan. F-prot can scan the entire system or folder, directory, files, CD-ROMS, network drives and it not only detects viruses or malicious files but asks to remove them if find them.

- **For Windows:**

  - **Total AV:** Total AV antivirus solution is a top-rated antivirus for windows operating system. TotalAV can deal with multiple viruses including malware, Trojan, spyware, and ransomware. As soon as the instance gets connected with any unknown threats, it first accesses it then downloads, installs, and checks for the consequences and harm it can do to the instance and issues warning and sometimes deletes it. If the website is harmful, it protects the instance by not showing the content of the website. Total AV comes with an option to schedule a smart scan. It also provides alerts for any kind of spam entry in mail server.
  - **ScanGuard:** ScanGuard is an effective solution which provides protection against malware, phishing attacks, Spyware. As it provides end to end security, one can get protection against data breaches and WebShield protections.

- **VirusFighter:** VirusFighter is providing Antivirus software solutions for Windows servers. It provides end to end security and monitors the environment, protection against corrupt webpages, security system protections and compatible with multiple platforms.
- **ClamWin:** ClamWin is an antivirus tool provides for Windows operating system and freely available give endpoint security to windows server. Clamwin is a freely available software solution and use ClamAv engine to find virus in the environment.
- **Window Defender:** Microsoft windows defender is freely available with Microsoft Windows operating system. It is an advanced next-generation protection provided by Microsoft to protect the endpoints in the cloud. Window defender allows to work in active or passive mode with any other antivirus application.

Test Conditions: All the tests on the Antivirus are conducted with some similar conditions. These are:

- Test before and after update: The Antivirus software tested just after the installations and after that the update command is executed to update the latest database. To check if any improvement can be observed.
- Test with increasing malware samples: The environment is fed with sample data one by one and check the efficiency in detection as well as scan the data in one go.
- Efficiency is checked by scanning the complete system and scanning only a folder.

After selecting free antivirus for both the cloud machine instances (Ubuntu and Windows) The next step is to compare each one of them by installing on the instances and then start the studies upon them. In the next section we will see the design and specification for this research.

4 Design Specification

To start the testing as mentioned in the methodology, two operating systems and some antivirus for both are needed. Similar approach for testing of each antivirus must be followed for unbiased evaluation. As shown in the figure 1 the architecture framework I am following in this project is quite simple and easy to detect the malware files.

The environment should be the same for both the operating platform and basic steps will be followed in the same manner. In the architecture diagram, antivirus is installed into the EC2 where application is running and scanning the whole environment. In the back of the scanning process the scanner is checking each of the file and its content and trying to match the signature that is already available in the local storage if not found it will check the signature in the repository that is available in web, if virus is not found in the scan the antivirus declare the file is safe and if in any case virus is found the file will send to the quarantine directory and full scan report is generated in the end of the process which can be read by the admin of cloud.

After EC2 installation, the first need to prepare the environment for antivirus. The virus files need to be added in the environment with some non-infected files, so in a

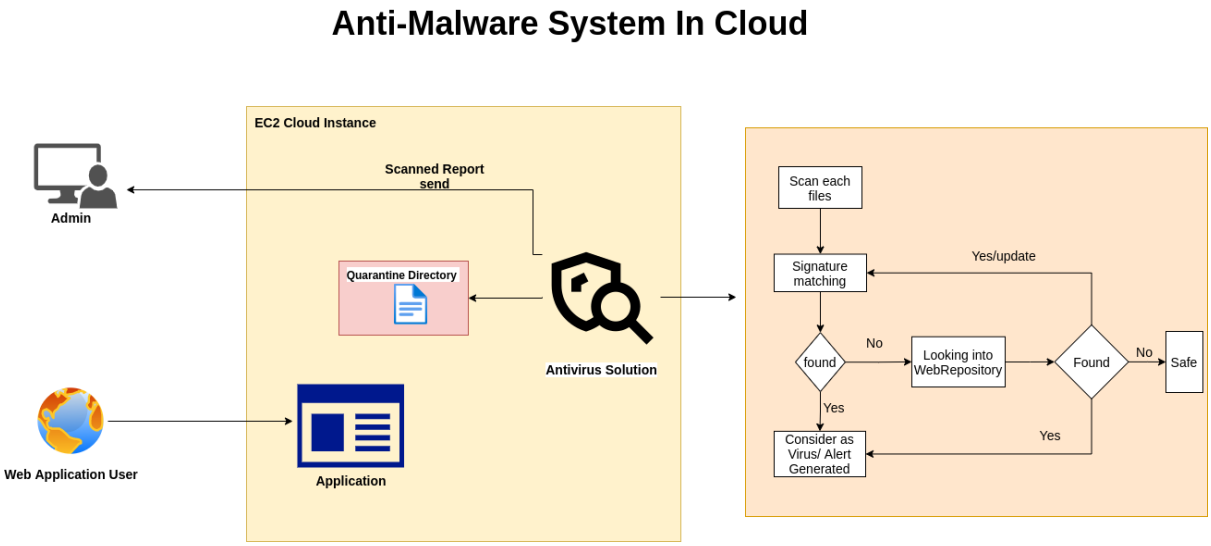

Figure 1: Architecture Diagram

directory this sample is prepared, so that after installation each antivirus can scan that folder and give the result. This mixture of files helps to test the false negative or false positive test. After doing this, each antivirus is installed with an on-demand scan option, so its performance will not be impacted by other antiviruses. It is necessary that if an antivirus found the virus in a file it should not be deleted, it can be quarantined or kept in that way. For the windows environment it is advisable to uninstall the first one antivirus and then install the other because, antivirus can have some performance issues, even if this is not the case then also other antivirus performance may get impacted by one another. In the next section the other specification of software and the operating environment is mentioned.

5 Implementation

To implement this research, the same architecture described in the design section is used. EC2 service of AWS is used to implement this project.

To start first it is needed to analyze the antivirus software and their software and hardware requirements, it helps in to select right machine to install each of the anti-virus. Table1 is showing System requirement to install mentioned antivirus software onto Ubuntu server.

5.1 EC2 Ubuntu Installation & Antivirus Testing:

To secure the application running on EC2 first an Ubuntu-18.04-x86_64 instance is needed to install chosen antivirus solution. The configuration for that is written in table 2 In the same EC2 instance some files including both corrupted and non-corrupted files are copied. To test the antivirus performance on the instance, some scenarios are made to check the performance.

As Ubuntu is the operating environment(non-GUI), all the antivirus is downloaded and installed with the help of terminal as well as the setting is done using the same.

Table 1: Ubuntu's Antivirus software configuration requirement

AntiVirus	Server Version	AMI	RAM	CPU	Version
ClamAV	Ubuntu 18.04 or higher	64-bit x-86 or 32 bit	3 GiB	1 CPU	0.103.6 /26734
COMODO	Ubuntu 16.04.2 or higher	64-bit x-86 or higher	284 MB	1 CPU	1
F-Prot	Ubuntu 16.04.2 or higher	64-bit x-86 or 32 bit	1GB	1 CPU	4.6.5.141
RootkitHunter	Ubuntu 18 LTS or higher	64-bit x-86 or 32 bit	1 GB	1 CPU	1.4.6
Sophos	Ubuntu 18 LTS or higher	64-bit x-86 or 32 bit	2 GB	1 CPU	9.12.1 2600654

Table 2: EC2 Machine Configuration

Host Machine	Values
Linux Kernel Version	Linux 4.15.0-196-generic x86_64
Operating System	Ubuntu-18.04-x86_64
RAM	4GB
VCPUs	2VCPU
Disk Size	40GB
Flavor	m1 medium

For each antivirus, the authorized site is used to follow instructions to download and install them. Most of the antivirus software allows upgrading their directories by using commands. The commands and testing methods of each antivirus are described below.

- **ClamAV:** ClamAV is an efficient tool to configure in your environment for protecting from viruses. For installation I followed the document available here.[1] Clamav can scan whole environment or just a specified folder by giving instructions in the command. It shows the output result on the screen and to get the output in the file we can give instructions accordingly. In the figure 2 the command is showing, which used to scan the specified folder and print the result in the log file and store log file in the mentioned directory.

```
ubuntu@x21153213-research:~$ sudo su
root@x21153213-research:/home/ubuntu# clamscan -v -l /tmp/clamavlog.txt -r /home/ubuntu/virus
Scanning /home/ubuntu/virus/ytisf-theZoo-7bff252.zip
```

Figure 2: ClamAV Command to Scan

  - -v: used to select verbose mode of output so that maximum information about the scan can be printed.
  - -l: to generate log file.
  - -r: to instruct the scanner about the directory which need to be scanned.

[1] `https://docs.clamav.net/manual/Installing.html`

- Freshclam: to update the database available for virus. It fetches the latest database.

- **Rootkit Hunter:** Rootkit Hunter scan for viruses and other security vulnerabilities. To install rootkit hunter, a document is followed [2] It provides detailed methods to install and configuration settings. Rootkit Hunter provides commands to update the data files. Scan command:

```
rkhunter --check
```

  After scanning the scan results save into

  var/log/rkhunter.log file.

- **COMODO:** COMODO antivirus is available for free, to scan for viruses, malware, email-filtering. To download and install on ec2 through command line, guidelines provided here are followed.[3]

  Scan command:

```
opt/COMODO/cmdscan -v -s /file/path
```

  -v: is verbose mode to get detailed report

  -s: to scan particular folder.

- **Sophos:** Sophos is a powerful tool to guard the system and is available free. To install Sophos, first need to download the sophos package in the local and then transferred it to the ec2 using scp command and then unzip the folder to start installation by going into the sophos-av directory and using sudo sh install.sh command. Sophos allow to configure email address also to send the alert message there.

  Scan command:

```
savscan -all /home/ubuntu/virus
```

  To check the logs Command is

  /opt/sophos-av/bin/savlog

- **F-Prot:** to install F-Prot on instance I followed steps mentioned in this document. F-Prot is considered as an efficient tool and can scan every kind of files including zip to match signature.[4] Scan Command:

```
fscan -a /root/to/directory
```

[2] https://www.vultr.com/docs/how-to-install-rkhunter-on-debian-10/
[3] https://learnubuntumate.weebly.com/comodo-antivirus.html
[4] https://www.howtoforge.com/f_prot_antivirus_ubuntu_feisty

5.2 EC2 Windows Installation & Antivirus Testing:

In the methodology section the antivirus solutions are mentioned. These antiviruses require some basic configuration which is available on the Table3 After analyzing the system requirement for the software solution, a window instance on AWS using EC2 service is created. Table4 shows Windows server configuration details.

Table 3: Window's Antivirus software configuration requirement

AntiVirus	Server Version	AMI	RAM	HardDisk	File Size	Version
ClamWin	Window Server 2003 or higher	64-bit x-86 or 32 bit	512 MB	512 MB	231MB	0.103. 2.1
ScanGuard	Windows7 or higher	64-bit x-86	2 GB	800 MB or higher	55.6 MB	5.19. 15.0
TotalAV	Windows7 or higher	64-bit x-86	2 GB	800 MB or higher	55.6 MB	5.19. 15.0
VIRUS-fighter	Window Server 2008 or higher	64-bit x-86 or 32 bit	128 MB	15 MB	2.30 MB	7.5.174
Windows Defender	Window Server 2008 or higher	64-bit x-86 or 32 bit	1GB	1 GB	115MB	1.379. 1039.0

Table 4: EC2 machine configuration

Host Machine	Values
Windows	Windows_Server-2016-English-Full-Base-2022.10.274
AMI	64-bit x-86
Operating System	Windows 2016
Instance Type	t2.micro
RAM	1GiB
VCPUs	1VCPU
Volume Size	30GiB

SetUp: After choosing above configuration for Windows EC2 connect local machine with EC2 remote instance using RDP Client by following document provided by AWS [5]

Remmina tool installed on Local Ubuntu system to access the windows instance using Remote Desktop Protocol. A Screenshot shows in figure 3 giving a view for configuration of connection. The work started after connecting the instance with local and setup a similar environment for this windows instance. Window provides GUI feature therefore I downloaded each free antivirus software one at a time and before doing that first disable Microsoft Window Defender which is in built antivirus provided by Microsoft to give additional security to windows users. It is observed that after disabling the defender, performance of instance is increased. For implementing the framework, one by one each antivirus is downloaded then installed.

- **TotalAV:** From the official site [6] of total AV download the software and install it. TotalAV provides multiple facilities and easy configurations to get maximum benefits. Some important features provided by TotalAV are:

[5] `https://docs.aws.amazon.com/opsworks/latest/userguide/workinginstances-rdp.html`
[6] `https://www.totalav.com/en/free-antivirus`

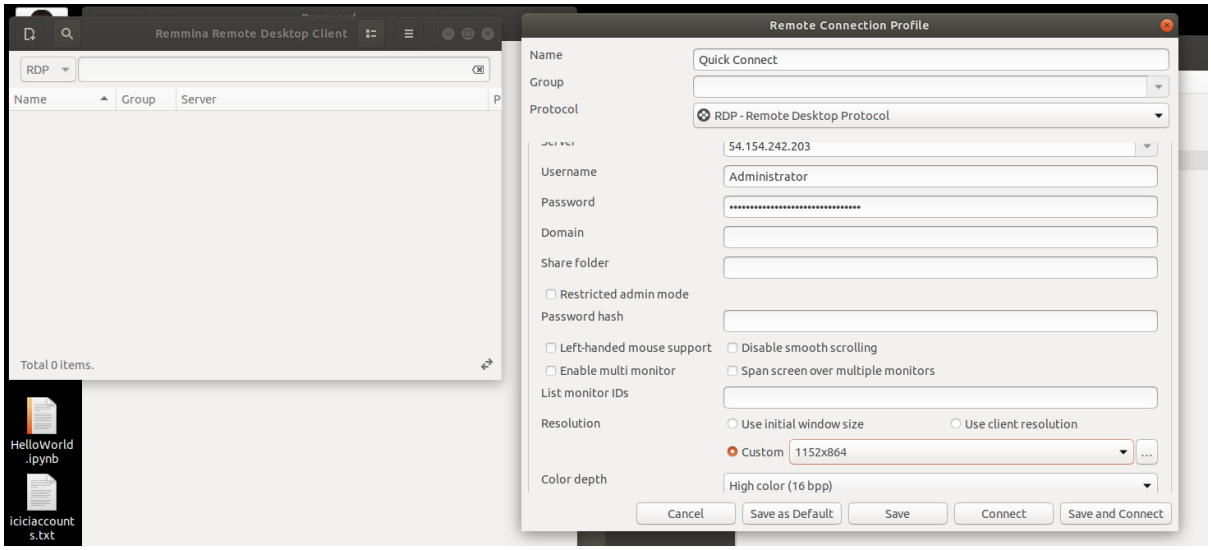

Figure 3: Remmina tool and configurations to connect with the instance

  - Scanning Files and folders: A setting can be done for files and folders and give directions to scan for files like .bin files or exe files, multiple file types can be given. The options for only scan documents or pictures/videos and another system files to ignore are available
  - Scanning Time: Customized schedule of scan can be configured by giving instructions to be active for time, even start and end time for scan can also be provided.
  - Notifications: Notification options are available to notify about scan start and end time and virus found or not found in scan by a small window. notification about web-shield feature use to block any webpage. notification about vpn connect. notification about when connected to insecure Wi-Fi network.
  - Web-Shield: set allow or not allow low trust websites, block cryptomining urls and it will check for such scenarios.
  - It updates its definition and check for updates in configurable time like each 3hours to 24hours or disable this feature
  - Boot time enhancer: by scanning for some programs that can increase system boot time, it can alert users about their load time.
  - A verbose logging is provided, though it took more space of disk
  - A folder for restored quarantine files can be chosen where you want to put infected or suspicious files to look into, check quarantine files and delete or restored them accordingly, those files will be restored in the same folders
  - A data breach check is also possible by giving emails as input

- **ClamWin:** ClamWin is a free antivirus solution developed by an open-source community. It is a window version of ClamAV we used in Linux that means ClamWin uses same scanning engine used by ClamAV but not affiliated with ClamAV. The download link is available on official website of clam.[7]

[7] `https://clamwin.com/`

As it is a window version, the GUI is available for installation and setup. Anyone can choose at installation time to download the updated virus signatures. After installing the antivirus, it will automatically update its virus database. Scanning: ClamWin can scan directories, select folders, or files and even the instance memory. While scanning it first load the virus signature database and then compare files one by one for any matching. After completion of scanning, it gives a report about found virus, time it took to scan. It does not remove infected files automatically.

- **ScanGuard:** Scanguard is an antivirus build to provide security against removable and non-removable drives, it can scan zip files, one can run a schedule scan and file types that need to include in scanning. For installation, the software from the web browser is downloaded using link provided on Scanguard website.[8] Features:
  - It provides protection from web using web shield. One can enable/disable web shield, choose options to block low trust and cryptominig URLs.
  - Multiple notification options are provided. It notifies when start and end of scan, if any webpage found suspected, if VPN got connect or lost connections, connected wi-fi is suspicious.
  - One can update the virus definition in the selected time.
  - Find if junk files are found and ask for deletion, junk files are not virus but unnecessary files (duplicate files) wasting disk space.
  - A smart scan or custom scan can be configured to quick check for viruses.
- **VirusFighter:** VirusFighter is an antivirus provides security for server endpoints. Version 7.5.174 with size 2.25MB is downloaded. It requires 512MB of Ram and disk space of 150MB.[9] Features:
  - It provides protection against SPAM, Virus, SPYWARE, and scan removable plus non-removable drives.
  - You can change the settings to scan the file-types and add some more extensions to investigate.
  - Quick scan complete scan and manual scan can be done, in manual scanning folder or multiple folder can be selected to scan.
  - Scheduling can be done for scanning the environment in a scheduled time.
  - To update the virus signature update option is available.
  - Complete logs of the software is provided after running the scan.
- **Window Defender:** To test Window's self-security management select Window Defender from the start menu. By providing real time detection with always up-to-date virus definitions, Window Defender is very protective antivirus by default all the security access are provided by Windows server to make secure operations. Real time protection can be turn off/on. Features:
  - In the setting many options are provided to make system more secure. With real- time protection on, any malware cannot be installed or run in to the system.

[8] `https://www.scanguard.com/free-anti-malware`
[9] `https://www.spamfighter.com/VIRUSfighter/Download_Download_Server.asp`

– Cloud-based protection allow windows to send the information to Microsoft to check for the security threats, by turning on the automatic sample submission you allow windows to send suspicious file's sample to Microsoft.

– Notification feature helps to send notification about the threat and health checkup report of system and any threat related issue that can cause serious harm.

6 Evaluation

After Implementing different scenarios to test the antivirus performance for Ubuntu and Microsoft Windows we got results and based on those results we can discuss here the performance on different level. Due to different platforms and methods, software solution and even performance of both environment(antivirus) is different, therefore different metrics for both environments are designed.

6.1 Memory Size after Installation

The size AV software took after installation. Note that if the size after installation is too large, it will affect the performance of the main application in the same VM (Virtual Machines). This experiment is done for both the environment. Figure 4 shows

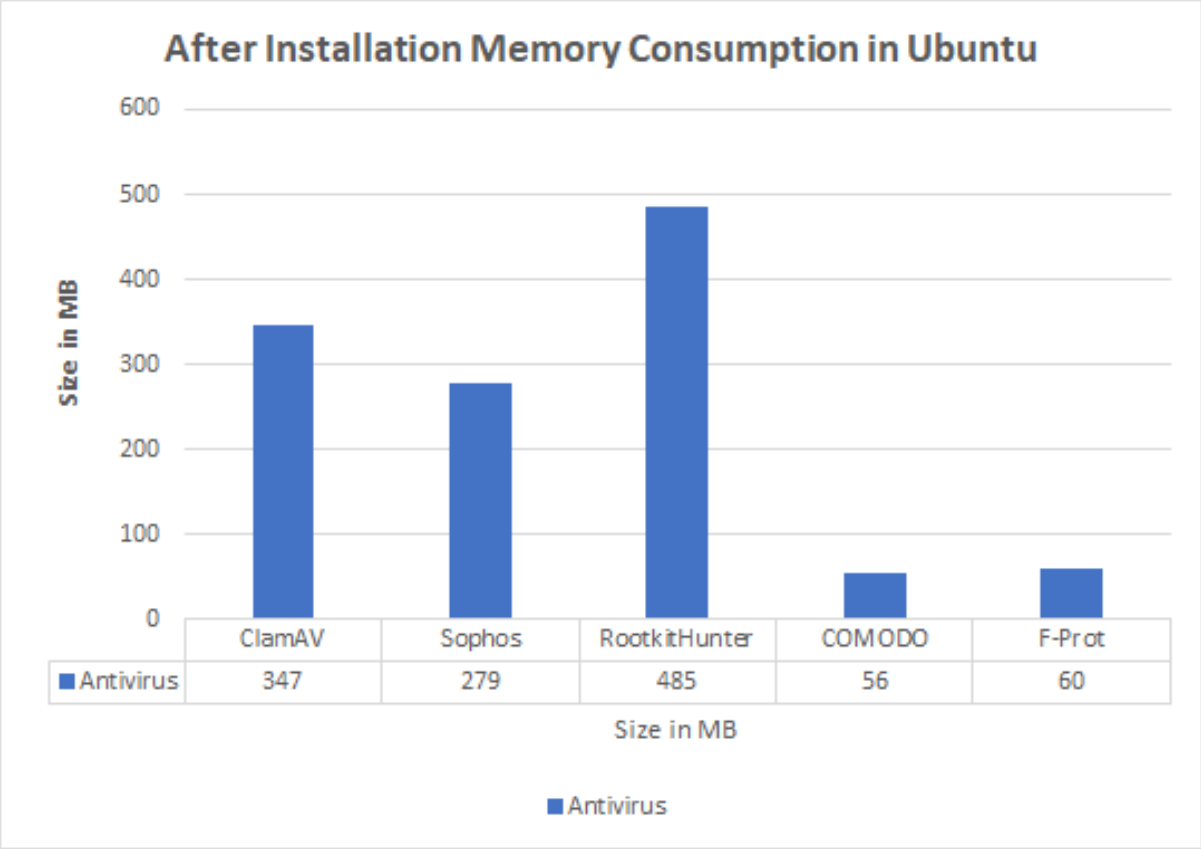

Figure 4: Memory Size comparison of Antivirus on Ubuntu

comparison between memory disk comparison of different antivirus after installation on

Ubuntu. Similarly in Figure 5 is showing comparison between memory disk consumption of different antivirus during custom scan and full scan on Window server.

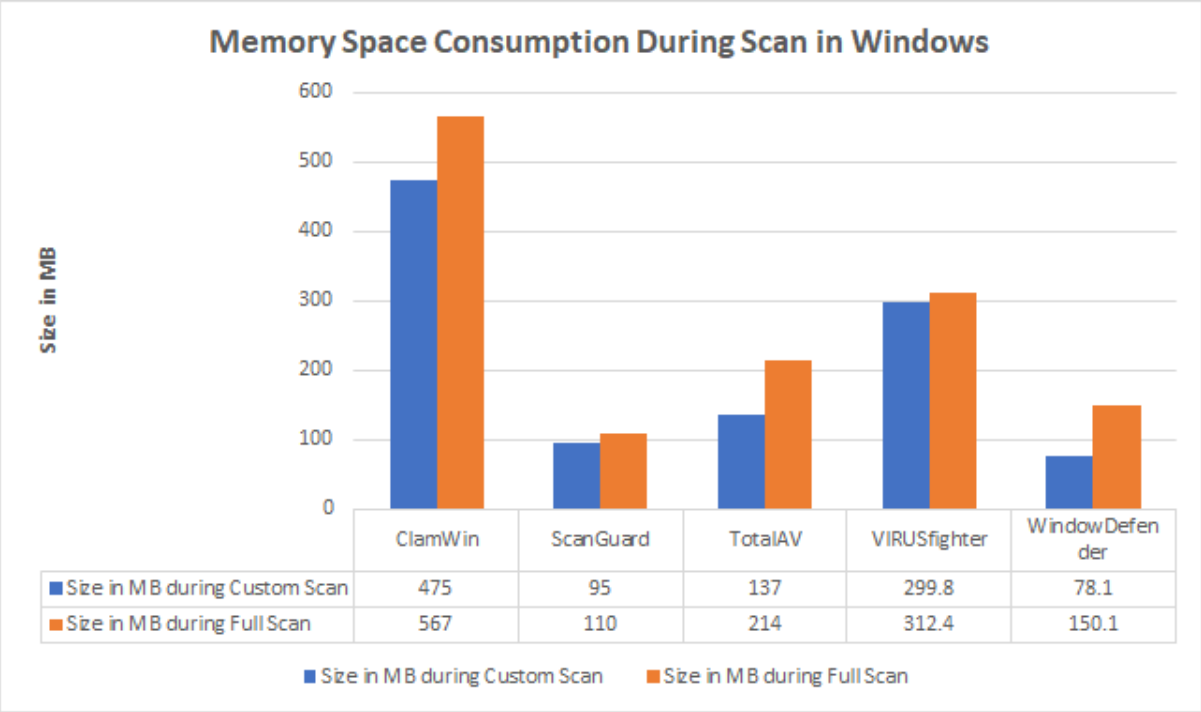

Figure 5: Memory Consumption comparison of Antivirus on Windows Server during custom and full scan

6.2 Scanning speed

How fast an antivirus can scan the whole machine is important. It can take a large amount of time and by measuring the speed we can configure the antivirus software accordingly like we can choose idle time for the machine.

This experiment is done for both the environment. Figure 6 shows scanning time taken by each antivirus solutions on Ubuntu server. Similarly Figure 7 is showing comparison between time taken by different antivirus during custom scan and full scan on Window server.

6.3 CPU resource Usage

How much CPU is utilized when scanning is in progress. It helps to think and target the task of scanning accordingly. If it took large amount of CPU the antivirus can only be scheduled when network is not busy or not receiving huge amount of traffic for the application or can say when application is not taking much CPU resources.

Figure 8 shows how much CPU is utilized during the process of scanning on Ubuntu. Similarly Figure 9 is showing comparison between CPU resource utilization during custom scan and full scan on Window server.

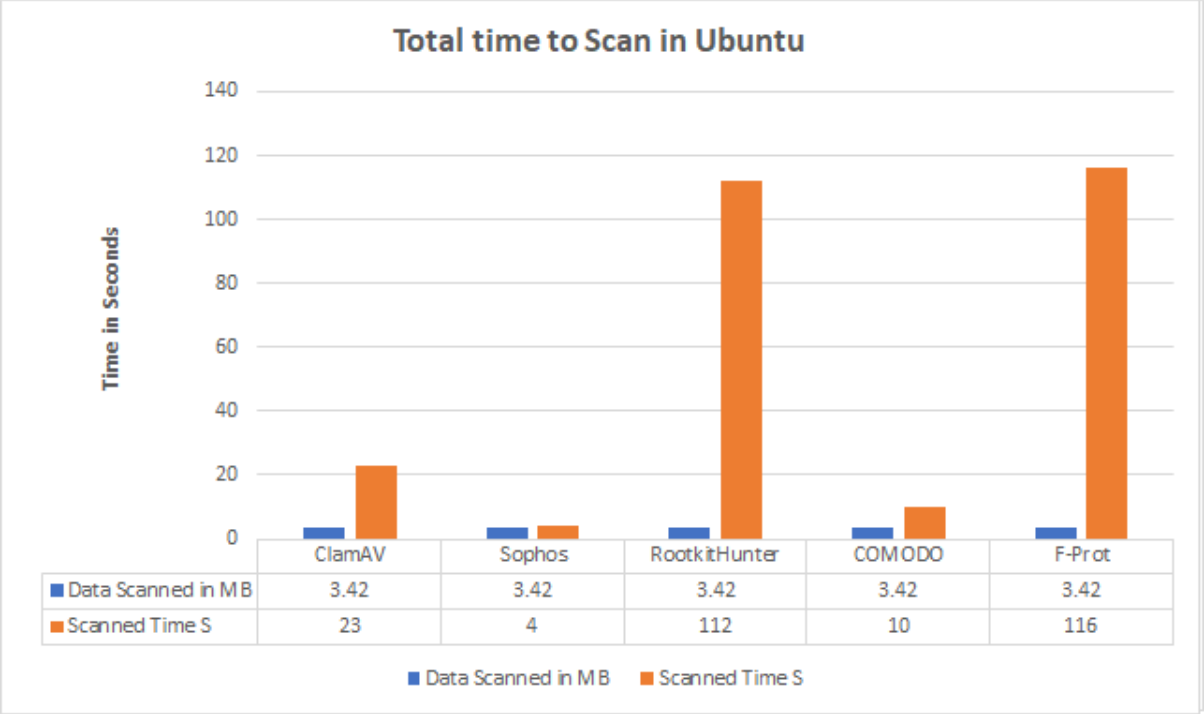

Figure 6: Time Taken by Each Antivirus on Ubuntu

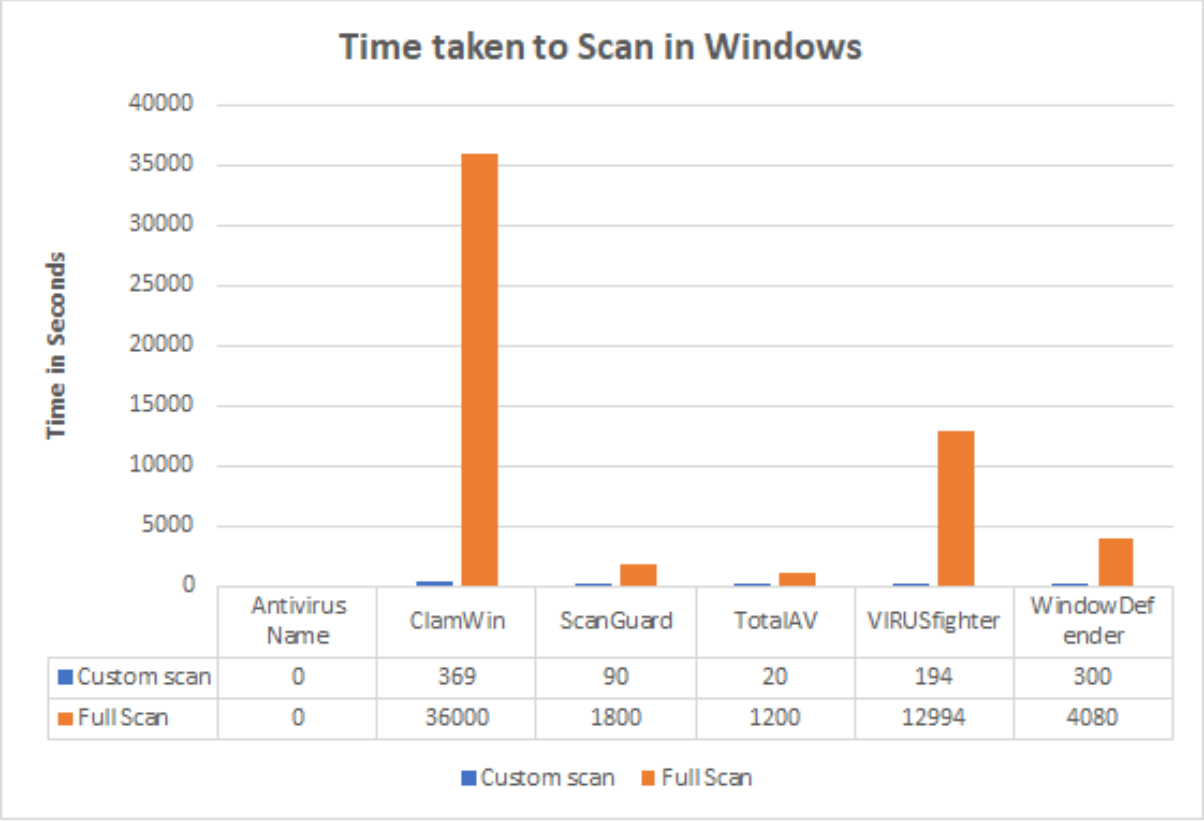

Figure 7: Scanning Time Comparison between different Antivirus on Window Server

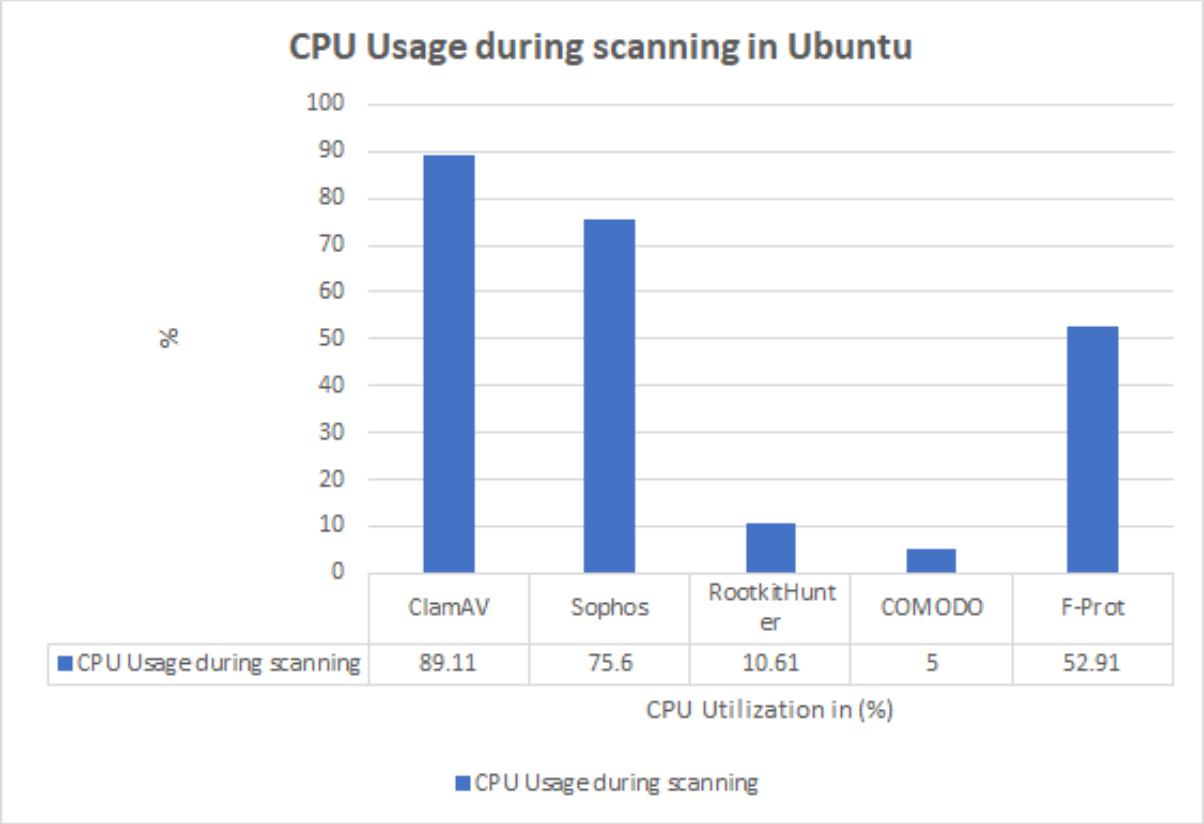

Figure 8: CPU Utilization during scanning on Ubuntu

6.4 Virus Definition Found

It is not necessary that every virus can detect all the signatures and find vulnerabilities in the system. After scanning, Antivirus solution generates output I save in the local and, based on that, concludes which solution is better. The table 5 and table 6 shows scanning results of different antivirus and their effectiveness in finding malware on Ubuntu and Windows server, respectively.

Table 5: Comparison between different Ubuntu Antivirus performance based on Scanning results

Criteria	ClamAV	Sophos	RootkitHunter	COMODO	F-Prot
Virus Found (in %)	80	70	Not Found	Not Found	95
Wrong Detection	NA	NA	NA	NA	1
Vulnerabilities Alerts	Available	Available	NA	NA	Available
Signature Detection	Found	Found	NA	NA	Found
Logging	Available	Available	Available	NA	Available
Found in multiple Scan	change found	NA	NA	NA	NA

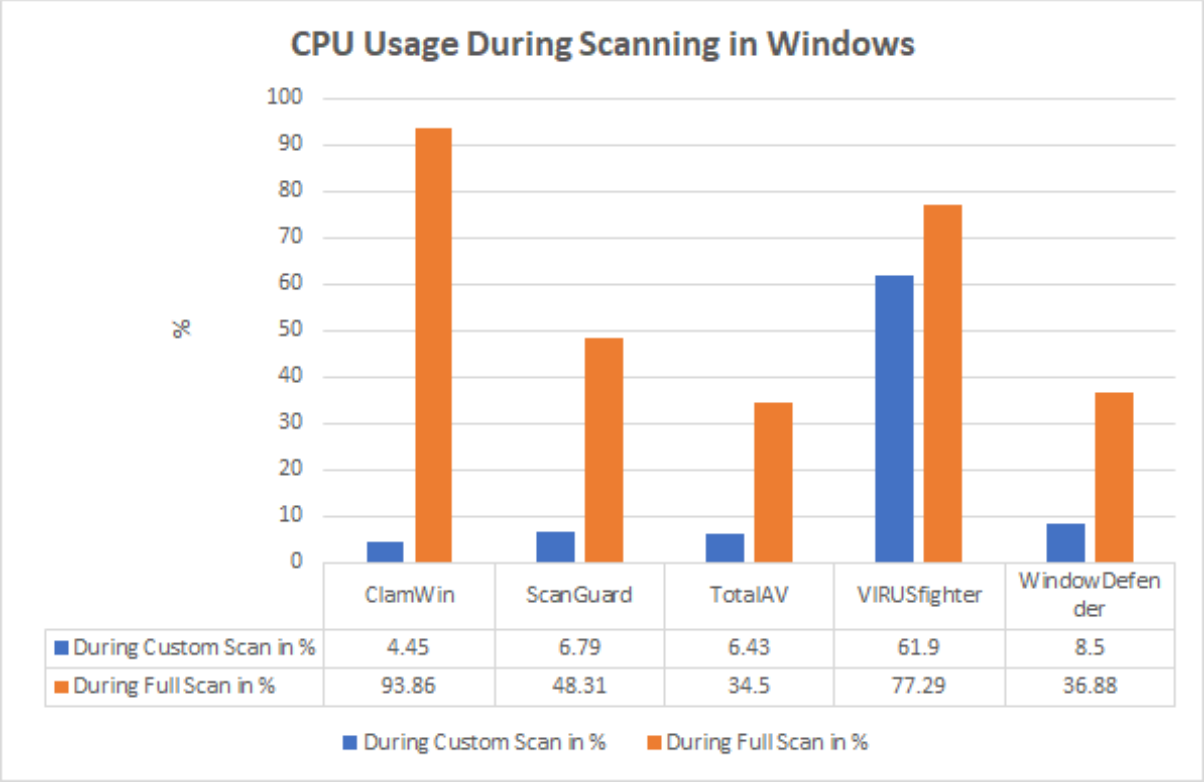

Figure 9: CPU Resource Usage Comparison between different Antivirus on Window Server

Table 6: Comparison between different Windows Antivirus performance based on Scanning results

Criteria	ClamWin	ScanGuard	TotalAV	VIRUSfighter	Window-Defender
Virus Found (%)	70	90	90	80	90
Wrong Detection	No	No	No	No	No
Vulnerabilities Alerts	NA	Available	Available	Available	Available
Signature Detection	Provided	Provided	Provided	Provided	Provided
UI Friendly (rate 1-5)	3	4	4	3.5	4.5
Multiple Scan	Same	Same	Same	Same	Same
Junk Files	NA	Available	Available	NA	Available
Web-Shield Protection	NA	Available	Available	NA	Available

6.5 Discussion

Based on the test conducted on both kinds of EC2 instances used to install antivirus solution to check the real-time performance of these Antivirus to effectively see the results

and decide to select from them.

- Antivirus should be tested on uniform platform. To maintain uniformity all the tests are revisited each time the antivirus is installed and all data about them is captured in the run time. In Ubuntu environment it was observed that some antivirus like COMODO and RootkitHunter though they are fast but not able to find corrupt files, because they are matching with extremely limited database available with them. On the other hand, in Windows platform after providing same scenario most of the antivirus can detect most of the virus except ClamWin as ClmaWin have very few abilities like it could not find vulnerabilities in the system and only match the signature that is loaded into the local database, though it can be updated but cannot detect run-time issues.

- To test the overall capability of antivirus, relying on some sample files can not give proper results. To address this issue multiple files are uploaded into the system and scan that folder multiple times. ClamAV at first cannot recognize one of the zipped files it detected in the second run. Even some files in the zip folder are showing okay in the scan while after extracting from zip folder the virus signature has been found. Figure10 and Figure 11 are giving a view that proves the ignored zipped file in the sample.

  Similarly in the windows platform many antiviruses give advantage to detect the virus at the run-time as soon as the suspected file reaches to the system. This functionality is tested by downloading some viruses at the run time if antivirus can give alerts. VIRUSfighter and Clamwin are the only viruses that do not provide these alerts in run time. No changes in detected malware are observed when providing the same data and scanning multiple times.

- In windows many of the antivirus solutions claim to provide protection against web threats. It is tested using multiple sites by visiting them and tried to download the content that is suspicious and note the results.

- The goal is achieved by using these viruses for over a month period and observe the performance and note the important points. To use the product in cloud it should be efficient enough to find the virus in the environment, If user is choosing Ubuntu or Linux as the platform, it is good to choose ClamAV or f-prot but according to observation F-prot is very efficient in finding vulnerabilities also but sometimes gives wrong results too, on the other hand ClamAV is efficient but consume a lot of resource which may affect the performance of real application. It is advised to set a cron job for the antivirus to handle such scenarios to schedule the job in the interval when overall processor utilization is low. On the other hand, for Windows, Windows Defender is a free and efficient antivirus which provide all kind of security but using real time detection for windows it also consumes a lot of resources and to deal with this one can get another less resource consuming solution like TotalAV which provides all effective detection with fast processing.

- After comparing on different criteria and utilizing the features provided the results are given in the table based on which anyone can take decision to use the correct solution. This will encourage users to not only use the antivirus but how effectively take the performance advantage of them in their secure cloud computing environment.

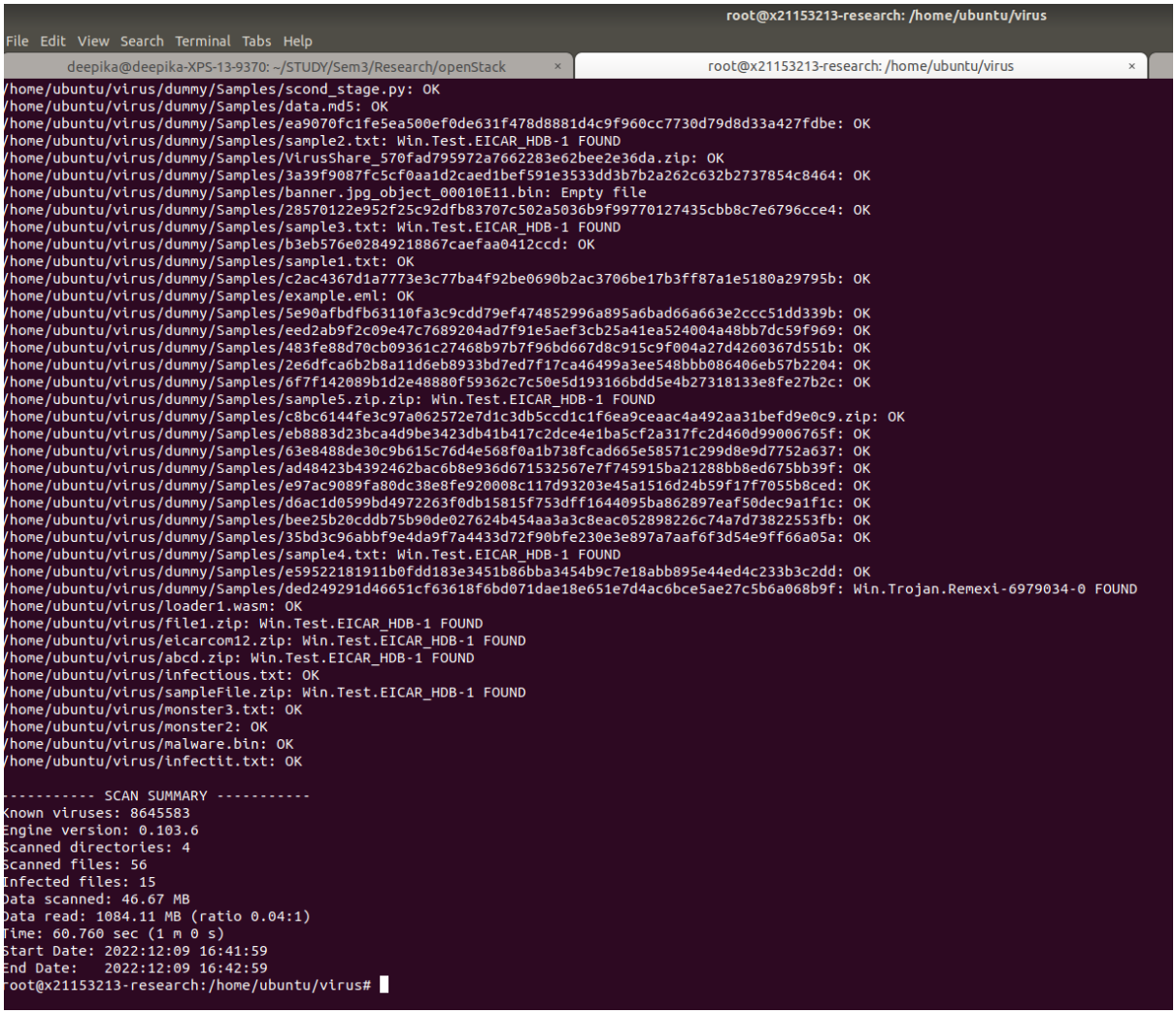

Figure 10: Overall Result

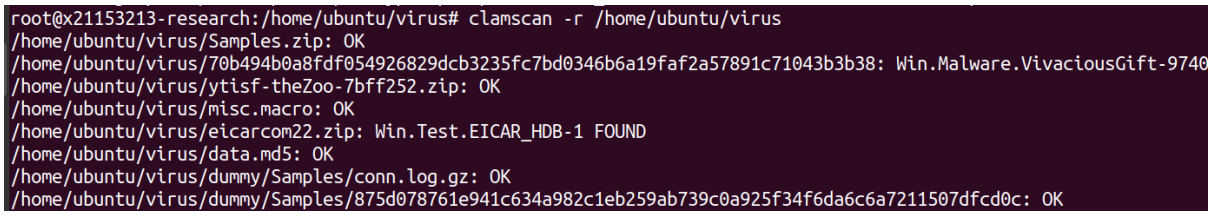

Figure 11: Focusing on the same zipped file with similar virus samples declared safe previously

7 Conclusion and Future Work

In this research first understood the need of antivirus in cloud computing and did the research around it to utilize the available solutions to improve security. Some solutions for Ubuntu and Windows are found. Before starting the implementation, sample malware from some repositories are collected. Some samples for window environment are downloaded at run time. This test-oriented approach helps me to test the run time evaluation of antivirus. Scanning multiple times for the same scenario ensures that the antivirus

updates themselves for new samples. After seeing the performances at each level, I come to conclude a scenario where the possible period can be adapted with chosen antivirus without impacting performance of application. These kinds of tests help me to accurately evaluate antivirus and fulfill the objectives of this research.
In future, this test can be performed with available antivirus services that can be plugged into the environment. One more metric which is not tested fully is to evaluate use of AI in antivirus solution to find the malware effectively. These tests were done with minimum resources, to use the recommended solutions in future, the user must test these with real-world applications they developed. This research will help to understand what the viable solutions will be according to their system or environment set up. Also, the chosen solutions are based on minimum requirement, if the user is selecting higher version architectures the solutions will behave in a better manner. This research focus is not about to find the preferable cloud architecture, however in the research I have found that if anyone is planning to get start with windows platform it is advisable to use a good antivirus solution which can protect as well as perform well.

References

Agrawal, A. and Wahie, K. (2016). Analyzing and optimizing cloud-based antivirus paradigm, *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, IEEE, pp. 203–207.

Botacin, M., Alves, M. Z., Oliveira, D. and Grégio, A. (2022). Heaven: A hardware-enhanced antivirus engine to accelerate real-time, signature-based malware detection, *Expert Systems with Applications* **201**: 117083.

Carstensen, J., Morgenthal, J. and Golden, B. (2012). *Cloud computing: Assessing the risks*, IT Governance Ltd.

Casey, P., Topor, M., Hennessy, E., Alrabaee, S., Aloqaily, M. and Boukerche, A. (2019). Applied comparative evaluation of the metasploit evasion module, *2019 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1–6.

Deshpande, S., Xu, C., Trochatos, T., Ding, Y. and Szefer, J. (2022). Towards an antivirus for quantum computers, *arXiv preprint arXiv:2203.02649* .

Dey, R. K., Roy, S., Bose, R. and Sarddar, D. (2021). Assessing commercial viability of migrating on-premise mailing infrastructure to cloud, *Int. J. Grid Distrib. Comput* **14**: 1–10.

Garba, F. A., Kunya, K. I., Ibrahim, S. A., Isa, A. B., Muhammad, K. M. and Wali, N. N. (2019). Evaluating the state of the art antivirus evasion tools on windows and android platform, *2019 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf)*, IEEE, pp. 1–4.

Hatem, S. S., El-Khouly, M. M. et al. (2014). Malware detection in cloud computing, *International Journal of Advanced Computer Science and Applications* **5**(4).

Leka, C., Ntantogian, C., Karagiannis, S., Magkos, E. and Verykios, V. S. (2022). A comparative analysis of virustotal and desktop antivirus detection capabilities, *2022*

13th International Conference on Information, Intelligence, Systems & Applications (IISA), IEEE, pp. 1–6.

Memos, V. A. and Psannis, K. E. (2015). A new methodology based on cloud computing for efficient virus detection, *New Trends in Networking, Computing, E-Learning, Systems Sciences, and Engineering*, Springer, pp. 37–47.

Nhlabatsi, A., Hong, J. B., Kim, D. S., Fernandez, R., Hussein, A., Fetais, N. and Khan, K. M. (2018). Threat-specific security risk evaluation in the cloud, *IEEE Transactions on Cloud Computing* **9**(2): 793–806.

Ongaro, T. O. (2020). *A compensatory approach to anti-virus shortfalls*, PhD thesis, Adventist University of Africa, School of Postgraduate Studies.

Raffa, G. (2021). Testing antivirus in linux: An investigation on the effectiveness of solutions available for desktop computers.

Salah, K., Calero, J. M. A., Zeadally, S., Al-Mulla, S. and Alzaabi, M. (2012). Using cloud computing to implement a security overlay network, *IEEE security & privacy* **11**(1): 44–53.

Santos, D. (2021). Comparison of paid subscription vs freeware software on antivirus program.

Sgandurra, D. and Lupu, E. (2016). Evolution of attacks, threat models, and solutions for virtualized systems, *ACM Computing Surveys (CSUR)* **48**(3): 1–38.

Sharma, Y., Gupta, H. and Khatri, S. K. (2019). A security model for the enhancement of data privacy in cloud computing, *2019 Amity International Conference on Artificial Intelligence (AICAI)*, IEEE, pp. 898–902.

Stange, S. (2015). Detecting malware across operating systems, *Network Security* **2015**(6): 11–14.

Updates, P. C. (2021). Antivirus software market growth driven by rise in cyber attacks worldwide — antivirus market valuation is expected to grow at a 10.8% cagr.

Yoo, S.-K. and Kim, B.-Y. (2018). A decision-making model for adopting a cloud computing system, *Sustainability* **10**(8): 2952.

Zeng, Y. G., Coffey, D. and Viega, J. (2014). How vulnerable are unprotected machines on the internet?, *International Conference on Passive and Active Network Measurement*, Springer, pp. 224–234.